UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

UNITED STATES OF AMERICA, Plaintiff, vs. ROBERT MYRON LATHAM, Defendant.	Case No. 2:06-cr-00379-LDG-GWF **FINDINGS & RECOMMENDATIONS AND ORDER DENYING *FRANKS* HEARING**

This matter is before the Court on Defendant Robert Myron Latham's Motion to Suppress Evidence (Franks Hearing Requested to Determine Whether Application for the Search Warrant Was Misleading) (#50), filed on October 9, 2007; the Government's Response to Defendant's Motion to Suppress Physical Evidence (#53), filed on October 19, 2007; and Defendant's Reply to United States' Response to Defendant's Motion to Suppress (#55), filed on October 25, 2007.

Defendant Robert Myron Latham is charged in a three count Indictment, filed on November 15, 2006, with transporting child pornography, receipt of child pornography and possession of child pornography in violation of 18 U.S.C. § 2252A(a)(1) (2) and (5)(B). Defendant argues that evidence seized from his computer pursuant to a search warrant should be suppressed because the affidavit in support of the search warrant contained material misstatements or omissions of fact. Defendant argues that if the complete facts had been included, probable cause would not have existed to support the issuance of the warrant. Defendant requests that the Court conduct a *Franks* evidentiary hearing to determine whether the alleged false statements or omissions in the affidavit were intentional or made

with reckless disregard for the truth, and if so, that the evidence seized pursuant to the warrant be suppressed.

FACTUAL BACKGROUND

On June 1, 2005, the Government applied to United States Magistrate Judge Lawrence R. Leavitt for a warrant to search the premises at 6420 East Tropicana Avenue, Unit 164, Las Vegas, Nevada and any computers located therein for evidence of child pornography as defined in 18 U.S.C. § 2256. *See Defendant's Motion To Suppress (#50), Exhibit "B", Attachment B.* According to the affidavit in support of the search warrant, a "growing phenomenon" on the Internet is "peer to peer" file sharing (P2P), which is a method of communication available to Internet users through the use of special software. *Id., Exhibit "B", Affidavit,* ¶ 14. As explained in the affidavit:

> Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up file(s) on a computer to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user's computer, and conducting a search for files that are currently being shared on the network. Limewire, one type of P2P software, sets up its searches by keyword. The results of the keyword search are displayed to the user. The user then selects file(s) from the results for download. The download of the file is achieved through a direct connection between the computer requesting the file and the computer containing the file. *Id.,* ¶ 14.

As further explained in the affidavit, a person interested in obtaining child pornographic images would open the P2P application on his computer and conduct a search for files by using a selected search term. The search is then sent out over the network of computers running compatible P2P software such as Limewire. The results of the search are returned to the user's computer and displayed. The user then selects which files he wants to download, which are then directly downloaded from the computer hosting the file to the area previously designated by the user for storage in his computer. *Id.,* ¶ 15. The affidavit also stated that a P2P file transfer is assisted by reference to an Internet Protocol (IP) address which is unique to a particular computer during an online session.[1] The IP address provides a unique location

[1]The affidavit also provides a general definition of "Internet Protocol address" or "IP address". *See Affidavit* ¶ 5.h.

making it possible for data to be transferred between computers. *Id.,* ¶ 17.

According to the affidavit, on February 25, 2005, FBI Special Agent (SA) Gordon, using an internet connected computer, launched the P2P Limewire program and conducted a keyword search using the term "r@gold" which is commonly found in the file names of child pornography images on file sharing networks. The result of the search identified 19 matching files which could be viewed and downloaded from the computer using the IP address 68.224.236.152. SA Gordon made a screen capture which displayed the name of these files, eight of which he determined had names indicative of child pornography. SA Gordon then used the Limewire "browse" function to view the names of approximately 270 image files stored in the share folder of the computer using the IP address 68.224.236.152. A review of the names of these files revealed that more than half of them had names indicative of child pornography. *Id.,* ¶ 23. SA Gordon then downloaded four image files from the computer using IP address 68.224.236.152, all of which contained images of child pornography. SA Gordon also attempted to download a fifth image, but more than half of that image was received from a different computer with a different IP address. *Id.,* ¶ 24. The four images downloaded by SA Gordon all contained depictions of child pornography as described in paragraph 25 of the affidavit. During the downloading process, the Limewire program displayed the source IP address of each image as 68.224.236.152. SA Gordon also used a software program called CommView which monitors internet and local network traffic and allows the user to view detailed IP address connections. This program also showed that the four images of child pornography were downloaded from the IP address 68.224.236.152. *Id.,* ¶ 26.

Pursuant to a search of the American Registry for Internet Numbers (ARIN), the Government determined that the IP address 68.224.236.152 is registered to Internet Service Provider (ISP) Cox Communications. The Government served an administrative subpoena on Cox Communications for subscriber information to IP address 68.224.236.152 during the time period that SA Gordon downloaded the images on February 25, 2005. Cox Communications' response to the subpoena listed IP address 68.224.236.152 as being used by the account of Larry Latham. According to the affidavit, Cox listed Latham's address as 6420 East Tropicana Avenue, Unit 164, Las Vegas, Nevada 89122 and also provided his telephone number and social security number. *Id.,* ¶ 27. Through checks of other public

data bases, phone company records and Nevada Department of Motor Vehicle records, the Government obtained additional information confirming that Larry Latham resided at 6420 East Tropicana Avenue, Unit 164. *Id.,* ¶ ¶ 28-30. On May 20, 2005, the Government again confirmed with Cox Communications by telephone that IP address 68.224.236.152 was assigned to Larry Latham's account from January 23, 2005 through May 20, 2005. *Id.,* ¶ 31. The affidavit further stated that physical surveillance of the residence, which is located in a mobile home park, was conducted on May 23, 2005, and a pick-up truck registered to Sherryl E. Carroll-Latham and a sedan registered to Larry Latham were observed at the residence. *Id.,* ¶ 32. Based on the foregoing information, Magistrate Judge Leavitt issued a search warrant on June 1, 2005 authorizing the Government to search the premises at 6420 East Tropicana Avenue, Unit 164, Las Vegas, Nevada 89122 and to search any computers and associated storage devices found on the premises for images of child pornography.

According to the Government, federal agents executed the search warrant on June 1, 2005. Investigation at the scene revealed that the residence was occupied by Larry Latham, his brother Defendant Robert Latham, and Sherryl Carroll. Pursuant to the search warrant, agents seized and searched two desk top computers belonging to Larry Latham and Sherryl Carroll. According to the Government, these computers did not contain contraband. The federal agents also seized and searched a laptop computer located in the residence which belonged to Defendant Robert Latham. A forensic examination of this computer revealed a large number of child pornographic images, many of which were saved in well-organized folders labeled by name or category. *See Government's Response (#53)*, page 6.

Defendant argues that the affidavit in support of the search warrant omitted important information about IP addresses and how they relate to computers that may use an IP address at any given point in time. Defendant argues that if complete information had been provided in the affidavit, there would have been insufficient basis for the court to find probable cause that child pornography would be found on a computer located in the residence at 6420 East Tropicana Avenue, Unit 164, Las Vegas, Nevada 89122. In support of his Motion, Defendant has attached an affidavit by Adrian Mare, an expert in computer networking, computer forensics and electronic discovery. *Defendant's Motion to Suppress (#50), Exhibit "A".* Mr. Mare's affidavit makes the following points:

* Computers access the internet through connections or portals. Each of these portals or connections is assigned its own Internet Protocol (IP) address. Each time a computer accesses the internet, it is assigned an IP address;

* One way a computer user can gain access to an IP address is to become a subscriber to an Internet Service Provider (ISP), such as Cox Communications. Upon becoming a subscriber, the computer user is permitted to connect to the ISP's network by physically attaching a connecting device, a cable modem, to cables located in their residence or business.

* In order to allow multiple computers to access the internet under the same IP address, the cable modem may be connected to a router, or may itself function as a router, which serves as a gateway through which multiple computers could access the internet at the same time under the same IP address. The router could be a wireless device in which case, computers located within 300 feet of the wireless router signal could access the internet through the router and modem under the same IP address. The wireless router signal strength could be increased beyond 600 feet if additional devices are added. The only way to prevent sharing of the wireless router is to encrypt the signal and even then an individual can bypass this security using publicly available software.

* There is publicly available software on the internet which permits a computer to "spoof" or fake an IP address in another network. Through this software an individual can make it appear that he is using a specific router when he is, in fact, using a different router. Thus, when this person sends a message or information to another computer, the receiving computer will be unaware of the true IP address of the sending computer.

* There is also publicly available software which permits a computer to "spoof" or fake the media access control (MAC) number of the computer, modem or router, which would prevent the ISP, such as Cox Communication, from knowing who is actually using its network to access the internet.

Defendant has also provided an affidavit by Al Tobin, an investigator for the Federal Public Defender's Officer, who states that he has spoken to April Lindskog, the same representative of Cox Communications that the FBI agent spoke to on May 20, 2005. According to Mr. Tobin, Ms. Lindskog advised that Cox tracks its subscribers' internet network use based on the MAC addresses of the cable modem associated with the account and "that a cable modem registered for an account could connect to Cox anywhere that Cox provided service and that a customer's access to Cox was not limited by geographic location or address." *Motion (#50), Exhibit "C", Tobin Affidavit.* Mr. Tobin's affidavit also states that based on his personal observation, there are approximately sixty homes located within a 600 foot radius of the premises at 6420 East Tropicana Avenue, Unit 164, Las Vegas, Nevada.

DISCUSSION

In *Franks v. Delaware*, 438 U.S. 154, 98 S.Ct. 2674, 57 L.Ed.2d 667 (1978), the Supreme Court held that the Fourth Amendment entitles a defendant to challenge the validity of a search warrant

affidavit if the defendant makes a substantial preliminary showing that (1) the affidavit contains intentionally or recklessly false statements and (2) the affidavit purged of its falsities would not be sufficient to support a finding of probable cause. *See United States v. Martinez-Garcia*, 397 F.3d 1205, 1215 (9th Cir. 2005), *citing United States v. Reeves*, 210 F.3d 1041, 1044 (9th Cir. 2000). In making the initial determination whether a defendant is entitled to an evidentiary hearing, *Franks* states:

> There is, of course, a presumption of validity with respect to the affidavit supporting the search warrant. To mandate an evidentiary hearing, the challenger's attack must be more than conclusory and must be supported by more than a mere desire to cross-examine. There must be allegations of deliberate falsehood or of reckless disregard for the truth, and those allegations must be accompanied by an offer of proof. They should point out specifically the portion of the warrant affidavit that is claimed to be false; and they should be accompanied by a statement of supporting reasons. Affidavits or sworn or otherwise reliable statements of witnesses should be furnished or their absence satisfactorily explained. Allegations of negligence or innocent mistake are insufficient.

438 U.S. at 171.

Franks further stated that if the defendant makes a substantial showing that the affidavit contains intentionally or recklessly false statements, "and if, when the material that is the subject of the alleged falsity is set to one side, there remains sufficient content in the warrant affidavit to support a finding of probable cause, no hearing is required." *Id.,* at 171-172. On the other hand, if the remaining content is insufficient to support probable cause, then the defendant is entitled to an evidentiary hearing. *Id.* At such hearing, the defendant has the burden of proof by a preponderance of the evidence to establish that the false statements were deliberately made or were made with a reckless disregard for the truth. *United States v. DeLeon*, 955 F.2d 1346, 1348 (9th Cir. 1992).

As the Ninth Circuit recently reiterated in *United States v. Jawara*, 474 F.3d 565 (9th Cir. 2007), intentional or reckless omissions may also provide grounds for a *Franks* hearing. The Court stated:

> "A search warrant, to be valid, must be supported by an affidavit establishing probable cause." *United States v. Stanert,* 762 F.2d 775, 778 (9th Cir.1985). In *Stanert,* we applied the rationale of *Franks v. Delaware,* 438 U.S. 154, 98 S.Ct. 2674, 57 L.Ed.2d 667 (1978), to hold that a defendant could challenge a facially valid affidavit by making a substantial preliminary showing that "the affiant intentionally or recklessly omitted facts required to prevent technically true statements in the affidavit from being misleading." *Stanert,* 762 F.2d at 781 ("By reporting less than the total story, an affiant can manipulate the inferences a magistrate will draw. To allow a magistrate to be misled in such a manner could denude the probable cause requirement of all real

> meaning.") In addition, the defendant must show that the "affidavit, once corrected and supplemented," would not "provide ... a substantial basis for concluding that probable cause existed" to search defendant's residence. *Id.* at 782.

Stanert also states that in determining whether a defendant is entitled to an evidentiary hearing, "[c]lear proof of deliberate or reckless omission is not required. *See United States v. Chesner*, 678 F.2d 1353, 1362 (9th Cir. 1982). Such proof is reserved for the evidentiary hearing." 762 F.2d at 781. The search warrant affidavit in *Stanert* alleged that defendant's residence was being used as an illegal drug laboratory. The court found that defendant had made a substantial preliminary showing that the affidavit omitted material information regarding each of the key facts relied on by the government to support probable cause and that the nature of the omissions suggested that they were made intentionally or at least recklessly. Probably the most glaring example was the affiant's statement that an illicit drug lab had previously exploded at the residence. The affidavit did not inform the issuing judge, however, that defendant did not purchase or move into the residence until after that explosion. The court also held that if the omitted information had been included in the affidavit, there would not have been a substantial basis upon which to find probable cause. Defendant was therefore entitled to a *Franks* hearing to determine whether the officer's omissions were intended to deceive the issuing judge or were made with reckless disregard for the truth.

As *Stanert* indicates, the materiality of the omitted information in regard to probable cause is relevant to the defendant's initial preliminary showing that the omissions were made intentionally or recklessly. The Seventh Circuit has stated that Defendant "must offer direct evidence of the affiant's state of mind or inferential evidence that the affiant had obvious reasons for omitting facts in order to prove deliberate falsehood or reckless disregard." *United States v. Souffront*, 338 F.3d 809, 822-23 (7th Cir. 2003). In this latter regard, the nature of the omitted facts must be such that it is reasonable to infer that they were deliberately or intentionally omitted from the affidavit. *See e.g. Stanert, supra,* (advising judge about previous drug lab explosion, but failing to disclose that it occurred before the defendant owned or resided on the premises indicated at least a reckless disregard for the truth.) In this case, the Government's search warrant affidavit provides a fairly detailed description of the means and methods by which persons use the internet and peer-to-peer programs to exchange and download images of child

pornography. It is reasonable to infer that the FBI agents who prepared or assisted in preparing the search warrant affidavit understand how IP addresses function and the extent to which IP addresses indicate where a particular computer is located. The issue before the Court, therefore, is whether the alleged omissions here would have defeated probable cause had they been included in the affidavit and, if so, whether they sufficiently evidence deliberate falsehood or reckless disregard for the truth.

In *United States v. Kelley*, 482 F.3d 1047, 1050-51 (9th Cir. 2007), the Ninth Circuit recently reiterated the standards for determining probable cause as spelled out in *Illinois v. Gates,* 462 U.S. 213, 103 S.Ct. 2317, 76 L.Ed.2d 527 (1983). The court noted that these standards apply with equal force to cases involving child pornography on a computer. *United States v. Gourde,* 440 F.3d 1065, 1069 (9th Cir. 2006) (en banc). *Kelley* states:

> Thus, probable cause means a "fair probability" that contraband or evidence is located in a particular place. *Gates* 462 U.S. at 246, 103 S.Ct. 2317; *Gourde,* 440 F.3d at 1069. Whether there is a fair probability depends upon the totality of the circumstances, including reasonable inferences, and is a "commonsense, practical question." *Gourde,* 440 F.3d at 1069 (citing and quoting *Gates,* 462 U.S. at 230, 246, 103 S.Ct. 2317). Neither certainty nor a preponderance of the evidence is required. *Id.* (citing *Gates,* 462 U.S. at 246, 103 S.Ct. 2317).
>
> Normally, we do not "flyspeck" the affidavit supporting a search warrant through de novo review; rather, the magistrate judge's determination "'should be paid great deference.'" *Gourde,* 440 F.3d at 1069 (quoting *Gates,* 462 U.S. at 236, 103 S.Ct. 2317 (quoting *Spinelli v. United States,* 393 U.S. 410, 419, 89 S.Ct. 584, 21 L.Ed.2d 637 (1969)). In addition, the Supreme Court has reminded reviewing courts that "[a]lthough in a particular case it may not be easy to determine when an affidavit demonstrates the existence of probable cause, resolution of doubtful or marginal cases in this area should largely be determined by the preference to be accorded to warrants." *Gates,* 462 U.S. at 237 n. 10, 103 S.Ct. 2317 (quoting *United States v. Ventresca,* 380 U.S. 102, 109, 85 S.Ct. 741, 13 L.Ed.2d 684 (1965)).

In *United States v. Gourde,* 440 F.3d 1065, 1069 (9th Cir.2006) (*en banc*), the government obtained a warrant to search defendant's residence and personal computer for child pornography based on information in the affidavit that defendant had subscribed to and remained a member of an internet website which charged a monthly fee, and which advertised and allowed members to view and download both legal pornography and illegal child pornography. The affidavit also discussed the characteristics of persons who collect child pornography, including their general habits in retaining child pornography on their computers or elsewhere in their residences. The *en banc* majority held that the affidavit provided a

fair probability that defendant had downloaded child pornography from the website and retained it in his possession at the time the warrant was issued. The majority therefore held that the search warrant was supported by probable cause. Relying on *Gourde*, the court in *Kelley* similarly held that the government's affidavit provided sufficient evidence to provide probable cause to believe that defendant had knowingly received and possessed email communications with attachments containing child pornography images.

In this case, Defendant Latham does not dispute that there was probable cause to believe that the user of the computer from which SA Gordon downloaded child pornographic images on February 25, 2005 knowingly possessed such images on his or her computer and/or transferred images to others through the Limewire peer-to-peer program. Defendant Latham argues, however, that the alleged omissions in the affidavit were intentional or reckless because (1) the Cox internet computer connection to which Larry Latham was the subscriber could have been located at premises other than the address shown on the Cox Communication billing records; (2) computer users outside Mr. Latham's residence could have connected to the internet under IP address 68.224.236.152 by accessing the wireless router and modem in Latham's residence; or (3) that it was possible for other computer users, using different IP addresses, to "spoof" or fake the IP address assigned to Larry Latham and make it appear that their internet connections were through the IP address assigned to him. Defendant argues that these facts should have been included in the affidavit and would have shown that there was not a sufficient basis for probable cause to believe that the computer from which Agent Gordon downloaded child pornographic images on February 25, 2005 was located in Larry Latham's residence.

Before discussing these allegations, the Court addresses Defendant's argument in his Reply (#55) that the Court may not deny a *Franks* evidentiary hearing based on the factual assertions made by the Government in its Response (#53) regarding Special Agent Gruninger's or FBI headquarters' lack of knowledge whether an IP address can be spoofed. The Court agrees that if Defendant has made a substantial preliminary showing under *Franks*, the Court may not deny an evidentiary hearing based on the Government's contrary factual assertions which are not based on information set forth in the search warrant affidavit itself. As *United States v. Mejia*, 69 F.3d 309, 318 (9th Cir. 1995) states, the district court is required to conduct an evidentiary hearing when the moving papers filed in connection with a

pre-trial suppression motion show that there are contested issues of fact relating to the lawfulness of a search. The Government's representations regarding Special Agent Gruninger's or the FBI's knowledge of whether it is possible to "spoof" an IP address are more properly addressed in an evidentiary hearing if the Court otherwise determines that Defendant is entitled to one. The Government has also not submitted any affidavits to support the additional factual assertions made in its Response (#53). For that additional reason, it would also be improper for the Court to consider those factual assertions as grounds for denying a *Franks* hearing if Defendant has otherwise met the substantial preliminary threshold. If the Court grants an evidentiary hearing, then the Government will, of course, be entitled to present evidence at the hearing to rebut Defendant's assertions.

The Court first addresses Defendant's argument that Larry Latham's address listed in the Cox Communications subscriber records was not necessarily the address where the Cox internet communication equipment was located. The search warrant affidavit states that in response to an administrative subpoena for the subscriber information for IP address 68.224.236.152, Cox Communications identified Larry Latham as the subscriber and listed his address as 6420 East Tropicana Avenue, Unit 164. Cox also provided Mr. Latham's telephone number and social security number. *Affidavit,* ¶ 27. The affidavit also states that on May 20, 2005, Agent Gruninger confirmed with a Cox representative that IP address 68.224.236.152 was assigned to Mr. Latham on February 25, 2005 when Special Agent Gordon downloaded the child pornography from a computer using that IP address. *Id.,* ¶ 31. Defendant has not shown that these statements were untrue.

The affidavit also states that online checks of public information data bases identified Larry Latham as Lawrence E. Latham with the foregoing address and that telephone service was provided to Mr. Latham at that address. *Id.,* ¶¶ 28-29. In addition, the Nevada Department of Motor Vehicles listed 6420 East Tropicana Avenue, Unit 164 as Mr. Latham's address on his expired driver's license and also showed that he had a motor vehicle registered in his name at that address. *Id.,* ¶ 30. On May 23, 2005, the agents conducted physical surveillance at 6420 East Tropicana Avenue, Unit 164, identified it as a residential premises and observed Mr. Latham's vehicle parked in a common area across from the residence. The agents also observed a vehicle registered to Sherryl E. Carroll-Latham at the same address, parked in the carport of the residence. *Id.,* ¶ 32. The information provided in the search

warrant affidavit therefore indicated that Larry Latham resided at 6420 East Tropicana Avenue, Unit 164 and that it was not merely a billing address. Absent other contrary information, it is also reasonable to infer that Larry Latham's Cox internet communication service would be located at that residence.

According to the affidavit of Defendant's computer expert, Mr. Mare, when an entity becomes a subscriber or client to an Internet Service Provider (ISP), they are permitted to connect to the ISP's network by physically attaching a connecting device, i.e., a cable modem, to cables in their residence or place of business. *Motion (#50), Exhibit "A",* ¶ 6. Mr. Mare also states that the IP address is actually assigned to the cable modem or router used by the subscriber. *Id.,* ¶ 9. According to the affidavit of Defendant's investigator, Mr. Tobin, regarding his conversation with former Cox employee, Ms. Lindskog, she explained that a modem registered for an account with Cox could connect with Cox anywhere that Cox provided service. *Motion (#50), Exhibit "C",* ¶ 5. Although the affidavit regarding Ms. Lindskog's statements is hearsay and somewhat vague, it appears that Defendant is contending that Larry Latham or someone else with access to his cable modem could have connected the modem to the Cox system at a location other than Mr. Latham's residence. Assuming that this information is true and had been included in the search warrant affidavit, however, it does not eliminate the likelihood or fair probability that Mr. Latham or another person using his assigned cable modem would do so from the premises at 6420 East Tropicana Avenue, Unit 164, Las Vegas, Nevada.

Second, Defendant argues that there was insufficient evidence to believe that the computer from which child pornographic images were downloaded on February 25, 2005 was located in Mr. Latham's residence because it was possible for multiple computers users located within 300 or 600 feet of that residence to connect to the internet through a wireless router and modem located in Mr. Latham's residence. According to Defendant, any computer which connected to the internet through Mr. Latham's Cox Communication connection would be identified under IP address 68.224.236.152. Defendant argues that if this information had been included in the affidavit, probable cause would have been lacking and this supports the inference that the omissions were intentional or reckless.

The Fifth Circuit in *United States v. Perez*, 484 F.3d 735 (5th Cir. 2007), rejected this argument as sufficient to defeat probable cause. In *Perez*, a woman complained to the police that someone with the Yahoo ID "famcple" sent her an internet message containing child pornography. The police

forwarded the complaint to the FBI. Through a subpoena to Yahoo!, Inc. the FBI determined that on the dates the child pornography was transmitted, the computer used IP address 24.27.21.6. The FBI determined that this IP address was owned by Time Warner Cable and, through a subpoena to Time Warner, learned that the IP address was assigned to defendant. Based on this information, the FBI obtained a search warrant to search defendant's residence. Defendant argued that the "mere association between an IP address and physical address is insufficient to establish probable cause." In rejecting this argument, the Court stated:

> In this case it is clear that there was a substantial basis to conclude that evidence of criminal activity would be found at 7608 Scenic Brook Drive. The affidavit presented to the magistrate included the information that the child pornography viewed by the witness in New York had been transmitted over the IP address 24.27.21.6, and that this IP address was assigned to Javier Perez, residing at 7608 Scenic Brook Drive, Austin, Texas 78736. Perez argues that the association of an IP address with a physical address does not give rise to probable cause to search that address. He argues that if he "used an unsecure wireless connection, then neighbors would have been able to easily use [Perez's] internet access to make the transmissions." But though it was possible that the transmissions originated outside of the residence to which the IP address was assigned, it remained likely that the source of the transmissions was inside that residence. *See United States v. Grant,* 218 F.3d 72, 73 (1st Cir. 2000) (stating that "even discounting for the possibility that an individual other than [defendant] may have been using his account, there was a *fair probability* that [defendant] was the user and that evidence of the user's illegal activities would be found in [defendant's] home") (emphasis in original). "[P]robable cause does not require proof beyond a reasonable doubt." *Brown,* 941 F.2d at 1302.
>
> Perez also argues that evidence that illicit transmissions were made does not give rise to probable cause that physical evidence would be located at the residence. However, the New York witness stated that the images she observed appeared to be videos played on a television screen transmitted via a web cam. There was therefore a basis to believe that the suspect would have such videos in his residence. Moreover, Britt stated in his affidavit that, in his experience, persons interested in child pornography typically retain numerous images of child pornography as well as "material documenting the arrangements, the introduction, and tasks to consummate the acquisition of child pornography." Based on this information, there was probable cause to believe that physical evidence of violations of the child pornography laws would be located at 7608 Scenic Brook Drive.

Perez, 484 F.3d at 740-41.

The affidavit in this case contains similar statements regarding the characteristics of persons who engage in the collection and exchange of child pornography. *See Motion (#50), Exhibit "A",* ¶¶ 6-13.

Defendant argues that there is an additional basis to question or doubt probable cause based on

the potential for "spoofing" of Mr. Latham's IP address. Assuming that spoofing exists, this may be an additional discounting factor regarding the probability that the computer from which Agent Gordon downloaded child pornography on February 25, 2005 was located in Mr. Latham's residence.

The Court finds, however, that considering these factors separately or cumulatively, there still remains a fair probability based on the information contained in the affidavit that evidence of child pornography would be found on the premises at 6420 East Tropicana Avenue, Unit 164. In this regard, the evidence set forth in the affidavit sufficiently demonstrated that the computer from which the child pornography was downloaded was identified by the IP address assigned to Larry Latham. The information provided by Cox Communication listed Mr. Latham's address, and other information obtained by the Government and set forth in the affidavit identified that address as Mr. Latham's place of residence. The affidavit of Defendant's own computer expert indicates that cable modems are connected to the cables that an internet provider such as Cox installs in the subscriber's residence or place of business. These circumstances therefore provided probable cause, i.e., a fair probability that the computer from which the images were downloaded was located in Mr. Latham's residence. This evidence did not, of course, establish with certainty that the computer was located on those premises. It was possible that someone other than Larry Latham or a resident of his household had accessed the internet either through his wireless router or by "spoofing" his address in order to engage in the exchange of child pornography on the internet. Probable cause under the Fourth Amendment, however, does not require certainty or even proof by a preponderance that the evidence sought is located on the premises to be searched. *United States v. Gourde,* 440 F.3d at 1069.

CONCLUSION

The Court therefore concludes that if the affidavit for the search warrant in this case had included the additional information that Defendant contends should have been included, probable cause would still have existed that evidence of child pornography would be found on the premises. The Court therefore finds that Defendant has not made a substantial preliminary showing under the second prong of the *Franks* test. Because Defendant's argument that the omissions were intentional or reckless is premised on the inference to be drawn from their materiality to the issue of probable cause, the Court also finds that Defendant has not made a substantial preliminary showing that the omissions were made

intentionally or with reckless disregard for the truth under the first prong of the *Franks* test. Accordingly,

RECOMMENDATION

IT IS HEREBY RECOMMENDED that Defendant's Motion to Suppress Evidence (#50) be **denied.**

Based on this Recommendation, it is further ordered that Defendant's request for a *Franks* evidentiary hearing is **denied**.

NOTICE

Pursuant to Local Rule IB 3-2, any objection to this Finding and Recommendation must be in writing and filed with the Clerk of the Court within ten (10) days. The Supreme Court has held that the courts of appeal may determine that an appeal has been waived due to the failure to file objections within the specified time. *Thomas v. Arn*, 474 U.S. 140, 142 (1985). This circuit has also held that (1) failure to file objections within the specified time and (2) failure to properly address and brief the objectionable issues waives the right to appeal the District Court's order and/or appeal factual issues from the order of the District Court. *Martinez v. Ylst,* 951 F.2d 1153, 1157 (9th Cir. 1991); *Britt v. Simi Valley United Sch. Dist.*, 708 F.2d 452, 454 (9th Cir. 1983).

DATED this 1st day of November, 2007.

George Foley Jr.

GEORGE FOLEY, JR.
UNITED STATES MAGISTRATE JUDGE